REMARKS

By the above amendment, applicants have amended claims to define the invention more particularly and distinctly so as to overcome the technical rejections and define the invention patentable over the prior art. In addition, applicants thank the Examiner for the clear and understandable Office Action

1. **Claims 21 and 31 are rejected under 35 U.S.C. 112, second paragraph**
   Applicants have amended Claims 21 and 31 to correct the issue regarding the lack of proper antecedent basis of the claimed subject matter.

2. **Claims 21, 24-27, 29-31, 33-37 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ueshima (6,731,731) in view of Yu et al (6,067,621), in view of Tabuki (5,841,970) and in view of Le et al (2003/0105962).**

   Claim 21

   In the last O.A., the Examiner notes that Ueshima teaches that the portable mobile communication terminal is used to generate one-time password for a plurality of authentication system unites presented on the network. Applicants agree that there are similarity between applicants' and Ueshima's system. However, there are differences. For instance, Ueshima's one-time password is generated by the server and transmitted to the client device and the application server, i.e.,

   Ueshima (col. 3 lines 40-42):
   "...CTI server generates a password, (5) the password thus generated is transmitted to both the user and the service provider,..".

Thus, it is this reason that Ueshima doesn't need to conduct synchronization between the authentication authority and user's authentication client device.

In the last O.A., the Examiner also notes that Yu teaches the generation of the one-time password by conducting synchronization between the authentication authority and user's authentication client device. Applicants agree that Yu does have a teaching of conducting synchronization. However, there is a vast difference between applicants' and Yu's synchronization process. Yu's synchronization is a counter based system which is predictable, while applicants' synchronization is completely random. As a result, applicants' system can generate unpredictable one-time passwords.

Although Yu also teaches that the one-time password is determined based upon the random number and the counter value stored in the terminal (col. 5, lines 16-17), it may appear that Yu's one-time password is also unpredictable. By a close examination, applicants find that this random number is initialized as a predetermined random number (col. 4, lines 27-28). After each generation of one-time password, this random number value will be increased by 1 and acts as a counter (col. 10, lines 47-48, Fig. 6). As a result, Yu's one-time password is predictable, because the counter value is predictable.

In the last O.A., the Examiner also suggests that Ueshima teaches the use of Web services to authenticate user. Applicants do not agree with this viewpoint. Ueshima does not have any teaching about Web services as taught by Brown (2004/0199636) or discussed by applicants invention. Ueshima only refers to the authentication process applied to general WEB users. The concept of using Web services as the mechanism to authenticate user is foreign to Ueshima.

Thus, the combination of Ueshima and Yu's teaching will not produce a system to meet the requirement of Claim 21.

In the last O.A., the Examiner also notes that Tabuki teaches the use of verification server to alleviate the burden on the application server. Applicants agree with the Examiner's viewpoint. However, as mentioned before, the combination of Ueshima and Yu will not produce a system to meet Claim 21. Thus, the combination of Ueshima, Yu, and Tabuki will also not be able to meet the requirement.

In the last O.A., the Examiner further notes that although Tabuki does not mention the concept of gateway authority, Le does teach such a concept. By a close examination of Le's teaching, it is the applicants' humble opinion that Le does not teach how to use a mobile device to generate one-time passwords for the purpose of allowing the application server to authenticate a user's identity. Instead, Le's teaching is to facilitate the authentication of a mobile device itself in a 3G cellular system (abstract and paragraph 0011). Thus, it is impossible to combine Ueshima, Yu, Tabuki, and Le's teaching to produce an operative system to meet Claim 21. Even if they could be combined, it is inherent that by combining a large number (over three) references of prior art is evidence of unobviousness.

Claim 24

As has been mentioned above, Le does not teach how to use a mobile device to generate one-time passwords for the purpose of allowing the application server to authenticate a user's identity. Le's teaching is for a different field.

In the last O.A., the Examiner notes that the proxy described in Le may have a role of the gateway authority. However, by referring to Le's Fig. 1 and a quote from Le's Abstract,

"When a request for authentication of a mobile station is generated, a signaling protocol message is generated at a proxy of the access network

within which the mobile station is to be authenticated. Detection of the authentication request is made at the proxy, and a message is generated at the proxy which includes indicia associated with the authentication center associated with the access network.",

it appears that the role of the proxy is more like an authentication handler. That is the proxy composes a request message and forwards the message to the core network for authentication, i.e., Le (paragraph 0016):

"The proxy detects the request and forms a signaling protocol message to be forwarded on to the home network.".

Thus, the concept of the gateway authority is foreign to Le.

Claim 25

As has been mentioned above, Yu does not teach the generation of non-predictable one-time password. Yu's system is a counter based system (col. 10, lines 43-61). If the counter value is cracked, the one-time password generated by Yu's system will become predictable. Thus, applicants' invention utilizes a new principle of operation to strengthen the security of the one-time password.

Claim 26

It may appear that the combination of Ueshima and Yu can produce a system that meet Claim 26. As has been mentioned before, Yu's system is a counter based system. The one-time password generated by such a counter based system is predictable. Instead, applicants' invention uses a Diffie-Hellman type of algorithms, which involves the use of power and modular math operators for every authentication session. Thus, applicants' system is highly unpredictable. Thus, the combination of Ueshima and Yu will not able to produce a system to meet Claim 26.

Claim 27

Applicants agree that Yu does teach means to ensure the success of the synchronization for a counter based system. These means involve the insertion of the counter values in the password (col. 8, line 49-51), transmission of the counter values and passwords from the terminal to the server (col. 8, lines 51-53), recovery of the counter values, comparison of the counter value (col. 5, lines 26-27), and resetting of the counter values when the counter values are not the same (col. 5, lines 28-30). However, Yu's system does not generate a confirmation code to alert the user about the success or failure of the synchronization. The generation of a confirmation code to verify the status of the synchronization is foreign to Yu. Thus, Yu's system can not meet the requirement as described by Claim 27.

Claim 29

Applicants agree that Ueshima does teach means to use portable, hand-held devices for user authentication. However, Ueshima's one-time password can not be generated locally. Instead, it is generated by the server and transmitted to the portable device (col. 3 lines 40-42). To generate one-time password by a portable or hand-held device is foreign to Ueshima. In contrast, the one-time password in applicants' system is generated independently and locally by the authentication device and the authentication authority, respectively. Furthermore, the independently generated one-time password does not transmit over the open air. Thus, for clarity, Claim 29 is amended to reflect the above mentioned argument.

Claim 30

Applicants agree that Tabuki does teach means to verify identities of any user or business by introducing the concept of verification server. However, Tabuki does not teach the use of one-time password for authenticating user and the use of gateway authority for balancing network load. Therefore, for clarity, Claim 30 is amended to stress the use of one-time password.

Claim 31

This is a system claim corresponds to method Claim 21. The same argument used in Claim 21 is also applicable to Claim 31.

Claim 33

This is a system claim corresponds to method Claim 24. The same argument used in Claim 24 is also applicable to Claim 33.

Claim 34

This is a system claim corresponds to method Claim 25. The same argument used in Claim 25 is also applicable to Claim 34.

Claim 35

This is a system claim corresponds to method Claim 26. The same argument used in Claim 26 is also applicable to Claim 35.

Claim 36

This is a system claim corresponds to method Claim 27. The same argument used in Claim 27 is also applicable to Claim 36.

Claim 37

This is a system claim corresponds to method Claim 29. The same argument used in Claim 29 is also applicable to Claim 37.

Claim 39

This is a system claim corresponds to method Claim 30. The same argument used in Claim 30 is also applicable to Claim 39.

3. **Claims 22, 23, 32 and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ueshima (6,731,731) in view of Yu et al (6,067,621), in**

view of Tabuki (5,841,970) and in view of Le et al (2003/0105962) and further in view of Brown et al (2004/0199636)

Claim 22

Brown teaches how to use Web services for user to access DB2 data (paragraph 0044-0049). Claim 22 employs the same Web services technology for user to access global authentication service through the use of gateway authority and authentication authority. The inclusion of Web services in applicants' system can produce unexpected and synergetic results, because the use of Web services technology can lead to an easy integration of the authentication authority service. This will further lead to the prevalent adoption and use of the authentication authority system. Of being able to achieve synergism is one of many reasons that applicants' invention is unobvious.

In the last O.A., the Examiner notes that it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Brown with Ueshima, Yu, Tabuki and Le, since one would have been motivated to use Web services because Web services offers the dual promise of simplicity and pervasiveness. It is applicants' humble opinion that even if the combination of Brown, Ueshima, Yu, Tabuki, and Le can produce a workable solution to meet the requirement as described by Claims 21 and 22, the combination of a large number (over three) references of prior art is evidence of unobviousness.

Claim 23

Brown teaches how to use WSDL and UDDI to publish and discover DB2 data service (paragraph 0007). Claim 23 employs the same technology to publish and discover the global authentication service. Brown does not have any suggestion that WSDL and UDDI can be modified and applied to meet the requirement of Claim 23.

Claim 32

This is a system claim corresponds to method Claim 22. The same argument used in Claim 22 is also applicable to Claim 32.

Claim 38

In the last O.A., the Examiner notes that Brown teaches that HTTP basic authentication, SSL, and SOAP signature can be used to handle varying needs of security and authentication when HTTP is employed as the transport mechanism (paragraph 0043). Claim 38 does not claim the invention of SOAP, SSL and HTTP. Rather Claim 38 addresses the use of SOAP, SSL and HTTP in the applicants' authentication authority system. The use of SOAP, SSL and HTTP in the applicants' system can produce unexpected and synergetic results, because the adoption of industry standard can produce a coherent system which is compatible with systems developed by other vendors. As a result, the applicants' authentication authority system can become a widely employed system in the market place. This approach can produce synergism as well.

4. **Claims 28 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ueshima (6,731,731) in view of Yu et al (6,067,621), in view of Tabuki (5,841,970) and in view of Le et al (2003/0105962) and Ha et al (2003/0152254)**

Claim 28

Applicants have amended Claims 28 to narrow the scope of the claim. This amendment is added because in applicants' invention, the user's private identity is never transmitted over the Internet as can be demonstrated by the definition of XA as shown in Equation 1, the description of processes as shown in paragraphs 0062-0068, and the brief summary described in the Abstract.

In the last O.A., the Examiner notes that Ha teaches how to use user's fingerprint to authenticate user's identity. By a close examination, applicants find that there is

a difference of how the private/biometric identity is treated by Ha and applicants' invention. As shown in Fig. 2A (Ha) and a quote from paragraph 0015 (Ha),

"A client (a user's PC) sends a one-time template (OTT), which is a combination of fingerprint data with a random OTT key transferred from an authenticating server, to the authenticating server;",

it can be realized that the fingerprint data in Ha's invention is actually transmitted over the wire. Although Fig. 2A shows that the OTT data is encrypted before the transmission, it is still a fact that user's private identity is transmitted from the client device to the server over the wire. In contrast, the private identity in applicants' invention does not have any risk of being exposed over the wire. Thus, applicants' invention takes a different approach to treat user's private identities. Therefore, the combination of Ha, Ueshima, Yu, Tabuki, and Le will not be able to produce a method or a system that meet Claims 21, 31, and 28. Furthermore, even if they could be combined, the combination of a large number (over three) references of prior art is evidence of unobviousness.

5. CONCLUSION

For all the above reasons, applicants' submit that the claims are now in proper form, and that the claims all define patentable over the prior art. Therefore, they submit that this application is now in condition for allowance, which action they respectfully solicit.

6. Conditional Request for Constructive Assistance

Applicants have amended the claims of this application so that they are proper, definite, and define novel structure which is also unobvious. If, for any reason this application is not believed to be in full condition for allowance, applicants respectfully request the constructive assistance and suggestions in order that this application can be placed in allowable condition as soon as possible and without the need for further proceedings.